INNOVATE. SUSTAIN. CREATE VALUE.

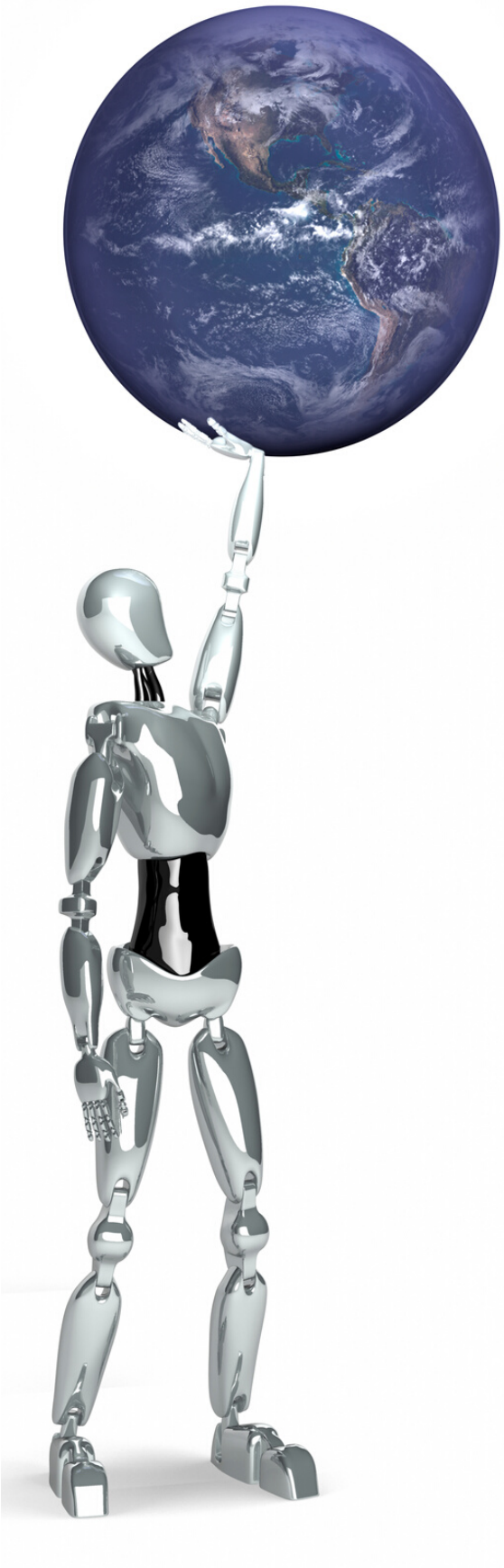
THE DCRO
RISK GOVERNANCE
INSTITUTE

EMBRACING TECHNOLOGY AND INNOVATION

A Cybersecurity Imperative for Every Board Member

Strategies to improve risk-taking
and risk-governance

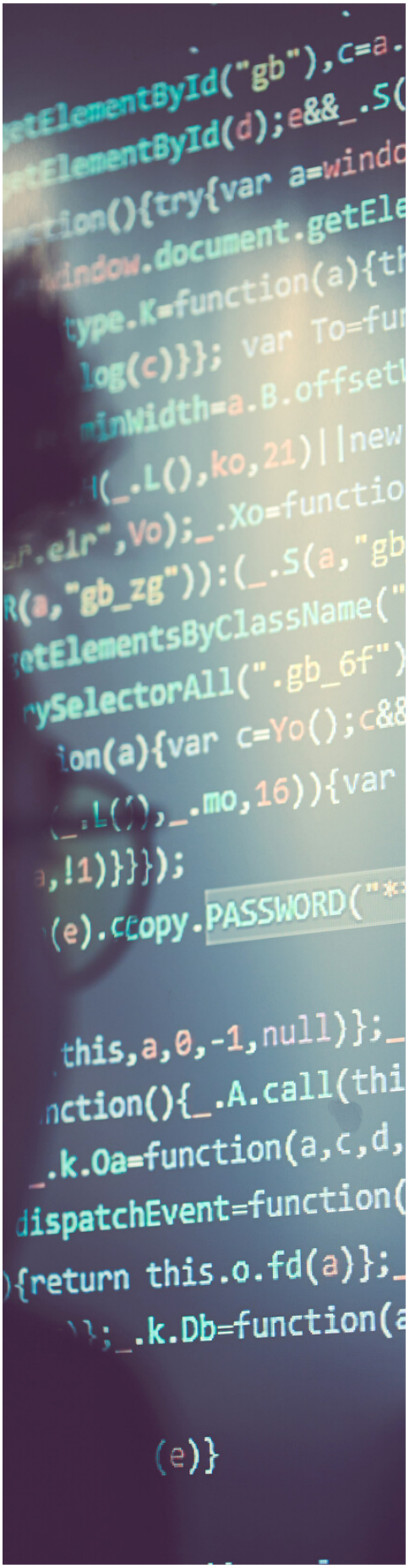
AN ESSENTIAL EMBRACE



An embrace of technology is essential for every organization that seeks to maintain relevance and market position. The success of that embrace depends not just on having the proper mindset and processes for innovation but on understanding how these new technologies impact all that constitutes the organization you govern. One key aspect of this impact is cybersecurity, making it imperative for every board director.

Like the need for innovation, cybersecurity affects companies across all industries, geographies, and stages of growth. Throughout the last decade, it has become essential for boards to understand technology and provide proactive oversight of its use. Cybersecurity's impact is far-reaching, touching every business area, from finance and customer success to public perception, data privacy laws, and more. Board directors today must not only be prepared to take on the complex responsibilities presented by cyber risk, but they must also approach it from an agile perspective as it is a rapidly ever-evolving space. And understanding gives companies a solid foothold to embrace technological innovation.

Conversations around cybersecurity emphasize the downside. Perhaps that's necessary to grab attention. Attacks *are* becoming more common; cybersecurity breaches have evolved from a fringe risk perceived to only harm companies



with inadequate protection to a probable event for companies with even the most significant resources and security expertise. Recent reports support the increasing severity and aggression in attacks:

- From 2020 to 2021, cybersecurity attacks on businesses increased by more than 15%.
- The average cyber breach cost a company nearly $9 million in 2020
- 88% of board directors see cyber security as a major business risk.
- There is no slowing down: 60% of executives predict cybercrime to continue to rise going forward

"Over the last five years, cybersecurity risk has been consistently rated among the top three business risks," says Homaira Akbari, experienced board director and CEO of AKnowledge Partners, LLC. "What is unique about cybersecurity is that sometimes a mundane cyber incident can result in massive business operations interruption and or undo a company's competitive advantage, for example through key data loss leaking highly sensitive information."

But we know with all risks that when we emphasize the fear of loss or the failure others have experienced, we alter how taking on those risks is evaluated – and not in a helpful way. Instead, it's best we take these serious and accurate statistics and turn them into realities that drive action, having the primary goal of those actions making our organizations more capable of embracing new technologies in our continuous evolution and advancement.

TODAY'S BOARD DIRECTORS REQUIRE FOUNDATIONAL CYBERSECURITY KNOWLEDGE

KNOWLEDGE BEATS FEAR

Fear is combatted by knowledge.

Companies that want to combat the potential for cybersecurity incidents and protect all stakeholders must first ensure the c-suite and board members have the knowledge they need, framed in a context that enhances fulfillment of their unique responsibilities. Ramy Houssaini, a Global Cyber Resilience Executive, says, "Cybersecurity should be treated with the same vigor, rigor, and quantification as any other business risk, and should not be looked at in isolation from the business and digital strategy of the company. Connecting the dots between the cyber risk profile and the business impact can only be achieved if the correlation between the two is fully understood."

Inherent to cybersecurity is the need to understand the board's and the company leaders' risk philosophy. Do they confidently embrace risk-taking, or are they more averse to doing new things? What is the broad risk management strategy, and does the company have the infrastructure to support that strategy? Have we planned and resourced the ability to respond when things are not as expected? And how does the board come together to collectively leverage risk to drive the business forward and create value?

Regardless of their functional background or areas of expertise, board directors must be prepared to address cybersecurity, including ensuring they consider cybersecurity within all board-level decisions. Whether an investment or acquisition, entering a new geographic market, integrating security into a product or buying process, or protecting customer privacy, you must consider the impact of cybersecurity. The responsibility sits with every board director, every leader, and every business unit.

STAYING ALIGNED: CYBERSECURITY AND BUSINESS STRATEGY

Ramy Houssaini

Homaira Akbari ,Ph.D

"A singular focus on compliance can be dangerous as it deprives the organization of looking at the opportunity side of cyber."

Houssaini cautions boards against getting too entrenched in fiduciary and regulatory mandates around cybersecurity and potentially losing sight of the business opportunity. "Cyber fatigue is real, especially in highly regulated industries," he says. "This creates, at times, a view at the board level that addressing cyber issues is mostly about compliance mandates. A singular focus on compliance can be dangerous as it deprives the organization of looking at the opportunity side of cyber when it comes to improving customer experience and the business resilience as well as augment the firm's competitive advantage."

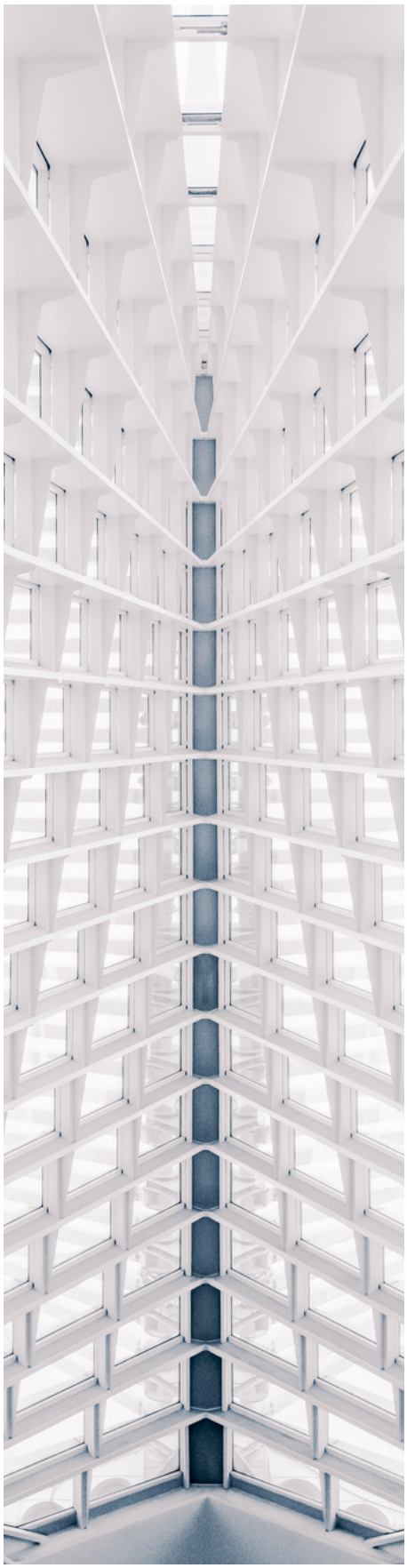
Akbari notes, "Companies should review their cybersecurity strategy, posture, and evolution at least twice a year at the board level. Best-in-class companies make this presentation at each board meeting. It is crucial that companies have a set of objective metrics which measure their cybersecurity maturity and that they share these metrics on a quarterly basis with their boards just like they do with their financials."

With such vast responsibilities in the cybersecurity realm, boards are responsible for ensuring the systems, structures, and relationships are in place to keep them reasonably in the know. One place to begin is by forming a relationship with a company's

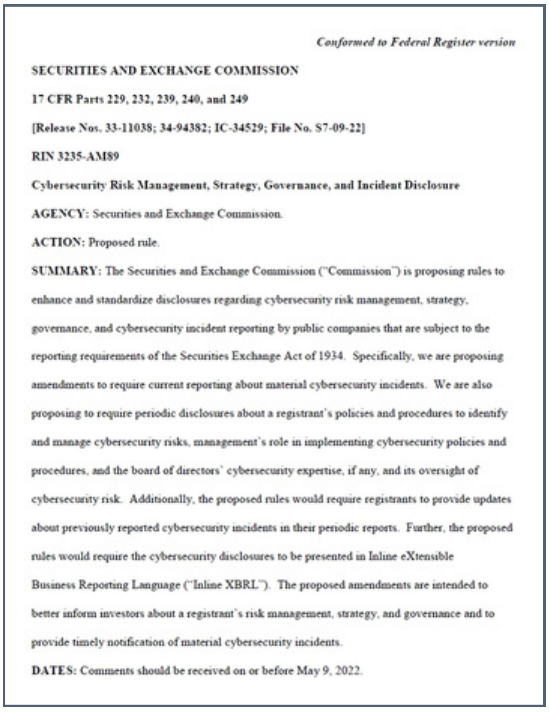
Chief Information Security Officer (CISO). The board can ensure that its overall strategic discussions align with the CISO's strategic plan for addressing cybersecurity, including lines of communication, reporting and tracking, understanding the customer impact, and communication with key parties. Importantly, they must know and communicate how to gauge success.

Some top questions or agenda items for boards to consider include:

- What are our current reporting structures and processes around technology and cybersecurity?
- Where are our current gaps and vulnerabilities?
- What resources do we need to overcome our current gaps and vulnerabilities?
- What is the current process for the flow of information, across teams, into leadership teams, and to the board, in the event of a cyber breach?
- What are the reports and metrics that we need to be regularly reviewing?
- Where are the gaps on the board in terms of cyber risk expertise?
- What does the board need to do to ramp up our knowledge and credentials to support the growing list of regulatory and investor disclosures and a potentially more robust cyber strategy?
- How do we always ensure that our technology spend aligns with and enhances our strategic plans?



AN EXAMPLE OF GROWING PRESSURE: NEW CYBER RISK DISCLOSURES PROPOSED BY THE SEC



Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is proposing rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents. We are also proposing to require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk. Additionally, the proposed rules would require registrants to provide updates about previously reported cybersecurity incidents in their periodic reports. Further, the proposed rules would require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL"). The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.

DATES: Comments should be received on or before May 9, 2022.

Proposed SEC Rule

It's no secret that boards are coming under even more scrutiny, not just in cybersecurity but in many technical realms. Not only do they have the fiduciary duty to oversee cybersecurity, but they must also be prepared to disclose their capabilities and vulnerabilities to the public. New proposed regulations from the Securities and Exchange Commission (SEC) could soon make cyber disclosures mandatory for companies listed in the United States. The SEC has proposed to require companies to disclose not only cyber incidents but risk management as it relates to cybersecurity governance, policies, and procedures and explain where cybersecurity sits within the overall business strategy. These disclosures also mean that companies must share individual board directors' cybersecurity oversight expertise, threat communication processes, the frequency with which that cybersecurity is on the board agenda, and more.

What's driving this? It's not just regulators. According to one study, 49% of CEOs globally are concerned about cyber risks, and 62% of employees and consumers perceive cybersecurity to be foundational to trust – and as we know, trust impacts the cost of all forms of capital upon which we rely.

At the same time, only 33% of board directors feel that they have a solid understanding of their companies' cyber vulnerabilities, according to a recent report from PwC. That's a gap that has to be addressed quickly. The means and opportunities to do so are available.

ENSURE YOU'RE PREPARED TO TAKE ON CYBERSECURITY OVERSIGHT

"Many board members don't have the appropriate grasp of what cybersecurity is," said Akbari. "The available literature is either too high level or too technical." Like many conversations around technical subjects, if there is a lack of understanding, there may also be a lack of necessary conversation, and there will certainly be a lack of ability to fully utilize the enormous impact an embrace of new technologies can have on our strategic evolution.

"Elevating the quality of the dialogues around cyber at the board level is possible if there is sufficient commitment to board cyber training, advised Houssaini." Cyber risks are unlikely to be transient business risks, so the investment in a deep understanding of the issues will pay dividends for organizations and board members."

Akbari agreed, saying, "It is essential for each board to have at least one director who is a cybersecurity expert, just like boards have directors who have audit committee financial experts. Additionally, it is paramount for other directors to get trained on cybersecurity at least once a year. Since cybersecurity is a hyper-dynamic field, the annual training provides the basis for non-cyber directors to understand the threat trends and the solutions to address these threats."

Houssaini took matters into his own hands when he approached the DCRO Institute about addressing this critical area. As the faculty member addressing Technology Risk Governance in The Board Members' Course on Risk®- the Institute's highly acclaimed risk governance program for current and aspiring board members, his vision was for a global program that gave board members the foundational knowledge they need, avoiding overly technical language and explaining in board language the technical issues around cybersecurity and technology in innovation.

The program he crafted with DCRO Institute President and Chief Executive Officer David R. Koenig brings together faculty from the board room, c-suite, military, law enforcement, and even former hackers. Collectively they convey the practical knowledge and tools needed for board members to fulfill their growing duty of care in this arena. Unlike many cyber risk courses, this one focuses on strategy and effective oversight. The order of those words in the course title, Cyber Risk for Boards: Strategy and Effective Oversight, is telling.

Among the faculty Houssaini assembled is Akbari, who sits on multiple boards and advises clients globally. Apropos of the DCRO Institute's core focus on the positive governance of risk-taking, her lecture is entitled, How to Safely Deploy Emerging Technologies, and features three case study interviews on how companies are actually using technologies like 5G, Artificial Intelligence, Blockchain, and the Internet of Things (IoT). The goal is to convey knowledge of how things are done well, not just to scare you with stories of all that has gone wrong elsewhere.

Fear can motivate. But more likely, fear will only motivate you to run. Knowledge, on the other hand, lets you embrace opportunities when others are not yet ready. Most boards know that to be the better approach to value creation and the opportunities to gain knowledge abound.

Educational Resources

- DCRO Guiding Principles for Cyber Risk Governance
- Foundations of Strategic Risk Governance
- Critical Risk Governance
- Resiliency and Effective Risk Governance
- A Successful Culture of Risk Governance
- The Board Members' Course on Risk®

TAKE A STEP FORWARD

Learn to embrace risk

To learn more about taking a positive approach to risk at the individual or board level, visit the DCRO Risk Governance Institute. For individuals, the DCRO can help you become a more strategic board director and contributor to corporate value with the globally recognized Certificate in Risk Governance®.

- Schedule a consultation
- Transform how your board engages risk
- Find a Qualified Risk Director®
- Enroll in our programs

THE DCRO
RISK GOVERNANCE
INSTITUTE

www.DCROI.org | info@dcroi.org | +1-612-286-1776